2025

SYNERGY
WEALTH MANAGEMENT

Senior Investors: Aim to safeguard yourself and your assets.

A guide for senior investors.

RON TARABORRELLI, CHFC®, CLU®, CFP®, EA
SYNERGY WEALTH MANAGEMENT LLC

Knowing and recognizing scams

Regulators and the financial industry are focused on senior investors—defined as those 62 and older by the NASAA Act—for a very good reason. Seniors have often accumulated significant wealth over a lifetime, which, unfortunately, makes them a prime target for financial scams and abuse. A report from the AARP Public Policy Institute found that 1 in 2 American adults report having been a victim or intended victim of financial exploitation[1]. This vulnerability is often compounded by age-related memory and judgment issues.

Having personally witnessed attempts to exploit older clients, I know how critical it is to be proactive. Fortunately, there are many steps you can take to help safeguard yourself and your assets. This guide is an excellent place to start.

A great way to protect yourself is to know what scams are out there.

1. **Romance scams.** Romance scams often begin on social media or dating apps. Scammers create fake profiles and invest significant time—sometimes months or even years—to build trust with their targets. They might message you for hours each day, working to establish a deep emotional connection.

   Once they have your complete trust, they'll create a story to ask for money, often promising to pay you back. These stories can vary widely:
   - **An Inheritance:** They might claim they need money to settle an estate before they can access a large inheritance.
   - **An Investment Opportunity:** They could present a "sure thing" investment and ask for a down payment, promising huge returns.
   - **A Personal Emergency:** They may pretend to be sick or need money for a child's medical treatment.

   A key red flag is that you've likely never met this person in real life. If they refuse a video call or make excuses to avoid one, it's a strong sign that something is wrong. The photos on their profile are often stolen from other people.

[1] AARP BANKSAFE™ INITIATIVE, How Banks and Credit Unions Can Better Serve and Protect People 50-Plus. Bank*Safe*™, June 2024 **© AARP PUBLIC POLICY INSTITUTE**

Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

2. **The grandparent scam**. In this scam, someone impersonates one of your grandkids, asking for money for rent, a car repair, or something else. In another version, someone acting like a person of authority calls like a police officer, offering to help your grandchild.
   As with most scams, they will pressure you to send the money quickly by playing on your emotions and creating a sense of urgency. Often, they will say something like they are embarrassed and ask you not to contact their parents or tell anyone.

3. **Tech support scams**. Unfortunately, I have seen many people fall victim to this scam, young and old. Typically, a person's computer or phone screen will freeze or go blank. A pop-up message will appear with a phone number to dial for help. When the user calls it, the scammer on the other end will ask for permission to log on to the device remotely. This fake "tech support" representative may also demand a fee to repair the "issue."
4. **Financial services scam**. In this scam, the call, text, or email appears to be legitimate and may appear to come from your bank, investment company, or even a debt collector. They will try to gain your personal information and can ask for your Social Security number or even passwords.
5. **Government impersonation scam**. This starts with someone claiming to be from the IRS, Social Security Administration, or some other government agency. They will try to scare you by saying that due to your unpaid taxes, we are about to freeze your assets, or that your Social Security payments are going to be frozen if you do not act.

   One thing to remember is that most government agencies **do not call you** they send notices through the U.S. mail.

Common ways to help protect yourself

1. Slow down, and if you find yourself getting emotional, end the interaction.
2. If someone claims to be from a government agency or financial institution, ask for the caller's information, like name and extension, and call the main phone number for that institution.
3. Never share your passwords or personal identifiable information.
4. Tell a trusted family member or friend and ask for help with the situation.
5. Ask for and obtain the person's name, telephone number, address, and business identity.

**********HELPING CLIENTS RETIRE WITH CONFIDENCE**********
Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

6. Never send money until you fully understand and are sure that it is not a scam.

Cyber Security

Seniors did not grow up with technology, and for some, it can be intimidating to learn and use technology. Scammers know this and try to take advantage of it. As companies increasingly use technology to engage their customers, seniors are being forced to adapt. Let's review the scams and how to protect yourself.

Phishing, Smishing, and Vishing

Phishing, smishing, and vishing are types of scams where a fraudster tries to trick you into providing sensitive personal or financial information by posing as an entity you know or trust, such as an investment firm, bank, or some other personal service that you use. The main difference between these "ishing" scams is the method the fraudster uses to try to steal your information or carry out other attacks. Phishing generally involves the use of e-mail; smishing involves the use of text or other types of direct messaging (e.g., messaging apps in various social media platforms); and vishing involves phone calls.

What type of information do these scammers want and why do they want it?

Fraudsters use "ishing" scams to steal personal information that may allow them to gain access to your e-mail, financial, or other accounts. Some of the information they may try to steal includes:

- Sensitive personal information (e.g., Social Security, driver's license or passport numbers)
- Bank, investment, or other financial account numbers
- ATM PIN numbers
- Usernames and passwords

What are some common characteristics of "ishing" scams?

Phishing scams involve fraudsters sending you e-mails to try and trick you into providing sensitive personal or financial information by having you reply to the e-mail, click on a

hyperlink to a website that mimics a legitimate website, or open an attachment that may download dangerous software to computer or mobile device. Fraudsters try to make these e-mails appear authentic by using:

- Names of real people, companies, or government agencies
- E-mail addresses that contain name of company or government agency
- Authentic-looking graphics and logos
- Links to webpages that appear to be a real company or government website
- Official-looking fine print and legal references

These e-mails also generally use an “urgent” message to try and solicit the information from you. Some examples of these messages include:

- Claims your account will be closed if you do not update your account information
- Alerts of suspicious activity in your account that ask you to verify your identity
- Claims of problems with your account or payment information
- Claims you have won a prize or money

Smishing scams involve fraudsters sending you texts or other direct messages to try to trick you into providing sensitive personal or financial information by having you reply to the text, or click on a hyperlink in the text that downloads dangerous software to your mobile device or takes you to a website that mimics a legitimate website. Fraudsters try to make these texts appear authentic by using names of real people, companies, or government agencies. These texts also generally use “urgent” messages similar to those used in phishing scams to try and solicit this information from you.

Vishing scams involve fraudsters using the same tactics used in phishing and vising scams except they call you on your home or mobile phone. Vishing fraudsters can make their calls look like they are coming from legitimate sources. These fraudsters also may learn some basic information about you from social media or other publicly available sources to make the call sound more legitimate.

Red Flags of “ishing” scams

Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

- Any request for personal or financial information – Use caution with any e-mail, text message, or phone call that asks you to provide any personal or financial information.
- Generic greetings, no greeting, and impersonators – These scams often target large numbers of people, so the text message or e-mail may use a generic greeting like “Dear sir or ma’am” or no greeting at all. Scam callers may ask to speak with “the head of the house,” or claim to be a representative from your investment or other financial firm, or from a government agency.
- Fear and Excitement – Fraudsters generally design these scams to prey on one of two powerful human emotions: fear or excitement. These emotions may lead you to make quick decisions without carefully considering your actions. This is why many of these scams involve either telling you something bad has or will happen, or that you have won something (usually money).
- Misspellings and bad grammar – E-mails and text messages associated with these scams often contain misspelled words and bad grammar. If you notice these types of mistakes in an e-mail or text message, treat your response to it with caution.
- Attachments and Hyperlinks – DO NOT open any attachment (e.g., pdfs, word processing and spreadsheet files, zip files) or click on a hyperlink in an unexpected e-mail or text message.

Protection Tips:

- Never provide personal or sensitive information via text message, e-mail, or to anyone on an unsolicited phone call.
- Never reply to any unfamiliar or unverifiable text messages or e-mails. Do not click any hyperlinks, open any attachments, or call back any telephone numbers in these messages. Fraudsters may be trying to see if a phone number or e-mail is active. By responding to the e-mail or text you have alerted the fraudster that they have a live target which may prompt additional e-mails and texts. Clicking on hyperlinks or opening attachments in these messages may also download dangerous software programs to your computer or mobile device that log your

Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

keystrokes and allow fraudsters to obtain usernames and passwords to your online accounts.

- If you receive a text message or e-mail from what appears to be your investment, bank or other financial firm, contact the firm directly through a verified telephone number to confirm that the information in the text or e-mail message is real.
- Immediately delete all suspicious e-mails and text messages.
- Enable multi-factor authentication for all your online investment and financial accounts.
- Download and install software and security updates for all your computers and mobile devices.
- Specific tips for Vishing scams:
    - Join the Do Not Call Registry.
    - Do not answer telephone calls from phone numbers you do not know. Let these calls go to voicemail. If the caller leaves a call back phone number in a voicemail, make sure you verify the phone number before calling it back.
    - If you accidentally answer a call from an unknown number do not respond to any prompts from the caller and hang up immediately.
- If you are a victim of any "ishing" scam, contact your investment, bank or other financial provider immediately and change the online passwords for your accounts.

Sorce: Investor Alert: Don't get "ished" – Tips to Protect Your Investment and Financial Accounts from Phishing, Smishing, and Vishing Scams | Investor.gov

Additional tips:

- Use a dedicated device for all your finances. Do not use the device for email or surfing the web.
- **Consider using a "strong" passphrase, instead of a password, if available.** Passphrases are passwords that consist of a series of words strung

together that create a phrase. Some investment accounts allow the use of passphrases, which generally require a longer character count than a password. A strong passphrase should consist of random words, using characters that include symbols, numbers, and both capital and lowercase letters. A strong passphrase should not use common phrases from literature, music, or other media. A strong passphrase also should not use personal information such as your name or birthday, or only words found in a dictionary. As with passwords, make sure you secure your passphrase, never share it via electronic messaging or over the phone, and change it regularly.

- **If you can't use a passphrase, pick a "strong" password, keep it secure, and change it regularly.** Select a strong password for your investment account. A strong password is one that is not easy to guess and generally uses twelve or more characters that include symbols, numbers, and both capital and lowercase letters. A strong password should not use words found in a dictionary, or personal information such as a name or birthday. Make sure you secure your password and never share it via electronic messaging (such as e-mail or text messages) or over the phone. You should change your password regularly.
- **Use two-step verification or "multifactor" authentication, if available**. Your investment firm may offer (or require) a two-step verification process for access to your account. Two-step verification is a practical way to add further security to your account by requiring a second factor to your username and password/passphrase sequence. With a two-step verification process, each time you attempt to log into your account from an unrecognized computer, your investment firm sends a unique code to either your e-mail or mobile device. Before you can gain access to your account, you must enter this code and your password.
- **Turn "on" account alerts.** One of the easiest ways to protect your online investment account and monitor it for fraud is to turn "on" account alerts. Depending on how your online account works, these alerts will send you an e-mail and/or text message when certain activities occur in your account. Some examples of these alerts include:

    - Account logins
    - Failed account login attempts
    - Password changes

- Personal information changes (address, e-mail or phone number)
- Securities transactions (placing orders to buy or sell investments)
- Transfers of money or securities in or out of the account
- Adding or deleting an external financial account where you can transfer money or securities to or from (e.g., bank account, investment account)

The availability and types of account alerts vary depending on your investment firm. Contact your investment firm to find out which online account alerts are available and how you can turn them "on" for your account.

- **Add biometric safeguards, if available.** Your brokerage firm or investment adviser may offer biometric safeguards for your online investment accounts, especially for access through mobile devices. Biometric safeguards for an investment account may include fingerprint, facial or voice recognition, or iris scanning. These safeguards may be used with or instead of a password/passphrase to access your investment accounts. Contact your investment firm to determine if they offer these safeguards for your accounts.
- **Use different passwords for different accounts.** Avoid using the same password for different online services, particularly for financial accounts. Using a single password for different online financial accounts is the equivalent of using a single key for your car, house, and mailbox – if the key is lost or stolen, you potentially give away access to everything. While using multiple passwords increases the difficulty of managing passwords, it significantly improves security.
- **Avoid using public computers to access your investment accounts.** Avoid accessing your investment accounts on a public computer, such as in a hotel business center or a library. If you must use a public computer to access your account, remember:

  - Avoid using public computers that require you to enter personal information in order to gain access.
  - Never walk away from a public computer while using it to look at investment or other financial account information. Leaving data up on a screen and walking away can enable potential onlookers to obtain your sensitive information.

- Disable password saving, and delete history files, caches, cookies, and temporary Internet files.
- When finished, log out of the account completely by clicking the “log out” button on the investment account website to terminate the online session. Closing or minimizing a browser application or window does not necessarily log you out of the account.
- Always change any passwords you have used on a public computer.

- **Use caution with wireless (or “Wi-Fi”) connections.** If you use a wireless connection to the Internet (including a wireless home network) to access your online investment accounts, make sure your computer or mobile device is secure and has current software updates, anti-virus software, and a firewall enabled. You can learn more about security issues relating to wireless networks on the website of the Wi-Fi Alliance at http://www.wi-fi.org/discover-wi-fi/security.

If you access your account on a public wireless connection, such as at a coffee shop or airport, you should use extra caution. It is very easy to “eavesdrop” on Internet traffic, including passwords and other sensitive data, on a public wireless network. If you use a public wireless network, remember:

- Do not type your password unless the website you are accessing uses a secure connection. The easiest way to determine whether a website is secure is to look in the address bar. If the page’s web address begins with “https” instead of “http,” then it is a secure connection.
- Turn off file sharing. With some operating systems, by default, all of your local files are wide open to any other device connected to the same network. Make sure this feature is turned off when accessing information over a public wireless network. You can usually find instructions for turning file sharing on and off in your operating systems’ help menu.
- Make sure the settings on your computers and mobile devices will not automatically connect to any available Wi-Fi connection. This will protect you from security risks in public spaces.

Update your devices and check your privacy settings.

- Make sure the software and software application (apps) on all your mobile devices and computers remain up-to-date with the latest software fixes and security patches.

Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

- Most software and apps have privacy settings for users which let you determine how much and what types of information are shared and stored. Always choose the least amount of data-sharing possible. *For any software and apps (including internet browsers), make sure they do not automatically save your account username and password.*

- **Be extra careful before clicking on links sent to you.** You should always verify that e-mails or text messages containing links regarding your investment accounts come from legitimate sources. Clicking on a malicious link could:

  - Link to a website designed to trick you into providing sensitive account information that can be used to steal your money or identity.
  - Cause malicious software (e.g., computer viruses, worms, Trojan horses, or spyware) to automatically infect your computer or mobile device and allow fraudsters to obtain sensitive account information.

To guard against dangerous links, remember the following:

- Do not click on a link that was sent to you by a business or entity you do not know. Perform an online search for the business or go directly to the business's website to determine if the link is legitimate.
- Do not click on a link that was sent to you by a business you use or know. Investors should confirm the legitimacy of the link by either going directly to the business's website or calling the business with a confirmed telephone number.

Source: Updated Investor Bulletin: Protecting Your Online Investment Accounts from Fraud | Investor.gov

Helpful websites:

FINRA.gov	NASAA.org
SEC.GOV	NCOA.ORG
Investor.gov	ALZFDN.org

**********HELPING CLIENTS RETIRE WITH CONFIDENCE**********
Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net

About Synergy Wealth Management LLC

At Synergy Wealth Management LLCWe recognize and appreciate the unique needs of our senior investors. That's why we prioritize a pressure-free environment, allowing you the time and space you need to make informed financial decisions. We strongly encourage and are happy to facilitate joint appointments with a trusted family member or friend.

Synergy Wealth Management is a qualified partner for your wealth management needs. You shouldn't have to feel uncertain about your finances. With over 25 years of experience, we provide tailored financial planning advice to help safeguard your future. Receive a personalized retirement and investment strategy. Schedule your Free Consult Today!

At www.synergywm.net

Schedule an appointment
Allow us to create a customized plan
Let's execute the plan together

My professional experience

My finance career began in 1996 as an insurance agent. I transitioned to investments and financial planning, primarily focusing on assisting clients with various investment goals. In 2008, I became an Enrolled Agent and established an income tax business. My expertise lies in holistic financial planning, encompassing retirement planning, income planning, tax-efficient asset management, annuities, and tax planning. I hold certifications as a CERTIFIED FINANCIAL PLANNER® professional, Chartered Financial Consultant, Certified Life Underwriter, and Enrolled Agent.

My personal life

I reside in the Philadelphia area with my wife, two daughters, and several pets. During the summer, we enjoy visiting the beach (Shore), and in the winter, we love skiing in the Poconos. I am an avid football fan and passionate about Philadelphia sports. Additionally, my wife and I take pleasure in savoring wine and exploring wineries.

Disclaimer: Investment advice offered through Stratos Wealth Advisors, LLC, a registered investment advisor. Stratos Wealth Advisors and Synergy Wealth Management are separate entities.

**********HELPING CLIENTS RETIRE WITH CONFIDENCE**********

Ronald Taraborrelli, ChFC®, CLU®, CFP®, EA
COO/Wealth Advisor. Direct: 856-562-8800
10000 Lincoln Dr. East, Suite 201, Marlton NJ, 08053
WWW.SynergyWM.net